

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MONTANA  
MISSOULA DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

vs.

BRYAN MICHAEL BALOG,

Defendant.

CR 23-45-M-DWM

OPINION and  
ORDER

Defendant Bryan Michael Balog is charged with receipt and transportation of child pornography in violation of 18 U.S.C. § 2252(a)(1), (2). (Doc. 1.) The charges arise out of Dropbox, Inc. reporting images of suspected child pornography in a CyberTip to the National Center for Missing and Exploited Children (“National Center”). (*See* Doc. 29-1.) Balog seeks to suppress the images on the basis that the National Center acted as a government entity or agent and its warrantless search of his private papers and effects violated the Fourth Amendment to the United States Constitution. (Doc. 28.) A suppression hearing was held on May 20, 2024, and the government called one witness, Missoula Police Detective Josh Harris. Having considered the parties’ filings, the record evidence, and the arguments at the hearing, Balog’s motion to suppress is denied.

## **BACKGROUND**

The factual background is taken from Detective Harris' testimony, as well as the exhibits attached to Balog's motion—Dropbox's CyberTip Report, (Doc. 29-1); a declaration by Dropbox Content Safety Manager Tobi Wulff, (Doc. 29-2); and Dropbox's Policies and Terms of Service, (Docs. 29-3 through 29-7)—and the government's exhibits—October 11, 2022 search warrant application, (Doc. 32-1); Dropbox preservation letter, (Doc. 32-2); and October 12, 2022 search warrant application, (Doc. 32-3).

### **I. Dropbox's Content Safety Review Process**

By federal statute, “[i]n order to reduce . . . and . . . prevent the online sexual exploitation of children,” electronic service providers such as Dropbox must make a report to the National Center of “any facts or circumstances from which there is an apparent violation of . . . child pornography [statutes]” “as soon as reasonably possible after obtaining actual knowledge of any [such] facts and circumstances.” 18 U.S.C. § 2258A(a); *see id.* §§ 2510(15), 2258E. The contents of that report are at the discretion of the provider, but may include, *inter alia*, email addresses, IP addresses, geographic information, and descriptions of the identified images. *Id.* § 2258(b). The National Center then forwards the CyberTip report to the appropriate law enforcement agency for possible investigation. *Id.* § 2258A(c). Dropbox, the provider at issue here,

provides an online file syncing and collaboration service that allows users to access and share their files on computer, phones, tablets, and the Dropbox website. When Dropbox users upload files to their Dropbox accounts, they can choose whether to keep files private within their accounts, to share their files with specified Dropbox users, or to share their files with the public by creating a “shared link.” Files that are shared publicly can be accessed over the Internet by any person who knows the Uniform Resource Locator (“URL”) for the shared link.

(Doc. 29-2 at ¶ 3.) Dropbox’s Acceptable Use Policy prohibits its services from being used to “publish, share, or store materials that constitute child sexually exploitative material (including material which may not be illegal child sexual abuse material but which nonetheless sexually exploits or promotes the sexual exploitation of minors), unlawful pornography, or otherwise indecent.” (Doc. 29-5 at 1.) Consistently, the Terms of Service explain that Dropbox may “access[], store[] and scan[]” user content and “may review [user] conduct and content for compliance with” its Terms of Service and Acceptable Use Policy. (*See* Doc. 29-3 at 1; *see also* Doc. 29-5 at 1–2 (reserving “the right to take appropriate action in response to violations of th[e Acceptable Use] policy, which could include removing or disabling access to content, suspending a user’s access to the Services, or terminating an account”).) Dropbox’s Privacy Policy further states that Dropbox discloses user information to third parties if it determines that a disclosure is “reasonably necessary to . . . comply with the law.” (Doc. 29-4 at 3.)

Consistent with the above, when Dropbox’s Content Safety Team becomes aware of potential child sexual abuse material, it removes the content and disables

the account if it determines that the content violates the Terms of Service and Acceptable Use Policy. (Doc. 29-2 at ¶¶ 7–8.) “When Dropbox discovers child pornography as defined in 18 U.S.C. § 2256, Dropbox provides a report to [the National Center] via the CyberTip in accordance with its statutory obligations under 18 U.S.C. § 2258A.” (*Id.* ¶ 9.) The Content Safety Team has been “trained on the statutory definition of child pornography and how to recognize it on our services. Dropbox makes reports in accordance with that training.” (*Id.*) Importantly, “[a]ll apparent child pornography is manually reviewed by a member of the Dropbox content safety team before it is reported to [the National Center]. This review is necessary for quality control purposes and to confirm the content to be reported qualifies as ‘apparent child pornography.’” (*Id.* ¶ 10.) “When Dropbox indicates in a CyberTip report that a file was “Reviewed by Company,” or otherwise states or indicates that Dropbox has viewed or reviewed the file, Dropbox is referring to a review of that image by a human reviewer prior to making the report.”<sup>1</sup> (*Id.* ¶ 12.)

## II. Balog’s Images

---

<sup>1</sup> This Court previously rejected an application of the private party search doctrine where the government failed to show what the private party did to “view” the images in the first instance. *See United States v. Weber*, 599 F. Supp. 3d 1025, 1036–37 (D. Mont. 2022) (describing this inquiry as “constitutionally significant”). Dropbox’s description of its process makes clear that the images were reviewed by an actual person before being reported.

On September 9, 2022, Dropbox provided a CyberTip Report to the National Center containing 40 files it had reviewed as potential child pornography. (Doc. 29-1 at 4–14; Doc. 29-2 at ¶ 11.) Dropbox categorized each image through a coding system that denoted whether a prepubescent or a pubescent minor was involved and whether the act depicted was a “sex act” or “lascivious exhibition”:

**The following categorization system was created by various ESPs in January 2014 and updated in June 2022:**

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2
Rank	Term	Definition	
1	Sex Act	<i>Any imagery depicting sexual intercourse (including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction of the above that lacks serious literary, artistic, political, or scientific value.</i>	
2	Lascivious Exhibition	<i>Any imagery depicting the lascivious exhibition of the anus, genitals, or public area of any person, where a minor is engaging in the lascivious exhibition or being used in connection with sexually explicit conduct, which may include but is not limited to imagery where the focal point is on the child's anus, genitals, or public area and where the depiction is intended or designed to elicit a sexual response in the viewer.</i>	

(Doc. 29-1 at 4–14, 15.) Using this system, Dropbox determined that most of the files were of prepubescent children: three files were classified as prepubescent children engaged in a sex act (A1), twenty-one as being a prepubescent child depicted in lascivious exhibition (A2), one as being a pubescent child engaged in a sex act (B1), and fifteen as being a pubescent child depicted in lascivious exhibition (B2). (*Id.*) Dropbox also provided information about the account that had uploaded the images, including the email address, a screen/username, a user ID, and the IP address for the upload device. (*Id.* at 3.) Upon receipt of Dropbox’s

report, the National Center manually reviewed only three of images, (*see id.* at 18), although all the images were automatically categorized through a “hash match” with known images of child pornography, and labeled as “Apparent Child Pornography,” “CP (Unconfirmed),” or “Child Unclothed.” (*See id.* at 16.) Using a publicly available IP address database, the National Center determined that they came from a Spectrum IP address in Missoula, Montana, (*see id.* at 15–17). The National Center forwarded the report and images to law enforcement in Montana. (*See id.* at 21.)

On October 11, 2022, Missoula Police Department Detective Josh Harris submitted a search warrant application to the state district court to review the 40 images based on the information contained in the CyberTip Report. (*See Doc. 32-1.*) A warrant was issued the same day. (*Id.*) Pursuant to that warrant, Detective Harris opened and viewed the 40 images underlying the Report and, on October 12, 2022, he applied for another search warrant from the state district court, this time to seize the data within Balog’s Dropbox account. (*See Doc. 32-3.*) According to the government, Detective Harris reviewed the data from Balog’s Dropbox account on October 24, 2022, and found over 1,200 images of child sexual abuse material. (*See Doc. 32 at 5.*)

#### **ANALYSIS**

“The Fourth Amendment guarantees the right to be free from ‘unreasonable

searches and seizures.’’’ *United States v. Rosenow*, 50 F.4th 715, 728 (9th Cir. 2022) (quoting U.S. Const. amend. IV). This right has two components, one property-based and one privacy-based. *See United States v. Wilson*, 13 F.4th 961, 967 n.7 (9th Cir. 2021). The former is ‘‘tied to common-law trespass’’ and focus[e]s on whether the Government ‘obtains information by physically intruding on a constitutionally protected area.’’’ *Carpenter v. United States*, 585 U.S. 296, 304 (2018) (quoting *United States v. Jones*, 565 U.S. 400, 405, 406 n.3 (2012)). The latter focuses on the ‘‘person’’ and protects an individual from unlawful intrusions into areas that an individual has a subjective expectation of privacy and that society is prepared to recognize as reasonable. *See Kyllo v. United States*, 553 U.S. 37, 33 (2001) (citing *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

Nevertheless, ‘[t]he Fourth Amendment regulates only governmental action; it does not protect against intrusive conduct by private individuals acting in a private capacity.’’ *Rosenow*, 50 F.4th at 728. Accordingly, ‘‘a private party may conduct a search that would be unconstitutional if conducted by the government.’’ *Wilson*, 13 F.4th at 967; *see Burdeau v. McDowell*, 256 U.S. 465, 475 (1921) (disregarding the private theft of papers used against a criminal defendant); *Coolidge v. New Hampshire*, 403 U.S. 443, 489 (1971) (holding that police need not ‘‘avert their eyes’’ when voluntarily offered critical evidence). A government

agent may then “reexamine” items previously discovered and revealed by a private party so long as the government agent does not exceed the scope of the private search: “[O]nce frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now-nonprivate information.” *United States v. Jacobsen*, 466 U.S. 109, 117 (1984).

“[A] private search or seizure may implicate the Fourth Amendment where the private party acts ‘as an agent of the Government or with the participation or knowledge of any governmental official.’” *Rosenow*, 50 F.4th at 728–29 (quoting *Jacobsen*, 466 U.S. at 113). “Whether a private party should be deemed an agent or instrument of the Government for Fourth Amendment purposes necessarily turns on the degree of the Government’s participation in the private party’s activities, a question that can only be resolved in light of all the circumstances.” *Id.* (quoting *Skinner v. Ry. Lab. Execs. Ass ’n*, 489 U.S. 602, 614–15 (1989)). “A federal regulatory scheme that authorizes and encourages private searches may transform a private search into governmental conduct.” *Id.* at 729. But “[e]ven if federal law does not render searches performed by private actors to be government conduct, a private search may still implicate the Fourth Amendment if there is a ‘sufficiently close nexus’ between the government and the private entity’s challenged conduct.” *Id.* at 731 (quoting *Jackson v. Metro. Edison Co.*, 419 U.S. 345, 351 (1974)). The relevant inquiry is “(1) whether the government knew of

and acquiesced in the intrusive conduct; and (2) whether the party performing the search intended to assist law enforcement efforts or further his own ends.”” *Id.* at 731 (quoting *United States v. Cleaveland*, 38 F.3d 1092, 1094 (9th Cir. 1994)).

Here, Balog argues that the National Center qualifies as a government entity or agent and, as such, violated his Fourth Amendment rights when it reviewed the files reported by Dropbox without a warrant. According to Balog, although the private party search exception may foreclose his claim under a reasonable expectation of privacy theory, *see Rosenow*, 50 F.4th at 732–33, it is inapposite under a trespass theory. Balog insists that electronic communications and images should be treated like traditional mail, maintaining their constitutional protections despite being deposited with a third party such as Dropbox. In response, the government argues that Balog’s position is foreclosed by the Ninth Circuit’s recent decision in *United States v. Phillips*, where the court held that “law enforcement officers do not violate the Fourth Amendment when . . . they mimic the trespass a private individual visited on another’s possessions after being alerted to the information uncovered pursuant to that trespass.” 32 F.4th 865, 874 (9th Cir. 2022). The government further argues that even if Balog is correct under a trespass theory, that does not undermine the evidence discovered in this case because: (1) law enforcement did not rely on the images reviewed by the National Center in seeking a warrant and (2) even if all the information regarding the

National Center was excised from the warrant application, probable cause would still have existed. Finally, the government argues that the “good faith” exception would apply. Because the government’s arguments have merit, Balog’s motion is denied.

## I. Burden

As an initial matter, two recent Ninth Circuit cases are inconsistent as to which party carries the burden in the private search warrant exception context. According to *Wilson*, a 2021 decision, “[t]he government bears the burden to prove [a] warrantless search was justified by the private search exception to the Fourth Amendment’s warrant requirement.” 13 F.4th at 971. However, under *Rosenow*, at 2022 decision, “[a] defendant challenging a search conducted by a private party bears the burden of showing the search was governmental action.” 50 F.4th at 729 (internal quotation marks omitted). Although not acknowledging this tension, the government appears to reconcile the two statements as follows: the government has the burden to prove its actions did not exceed the scope of an initial, private search, and the defendant has the burden to show that initial, private search was government action. (*See* Doc. 32 at 5–6.) This is consistent with the idea that the government bears the burden once the protections of the Fourth Amendment have been triggered. *See United States v. Tennant*, 2023 WL 6978405, at \*11 (N.D.N.Y. Oct. 10, 2023) (collecting cases regarding burden).

Accordingly, the government has the burden to show that neither it nor its agent exceeded the scope of Dropbox's initial search and Balog has the burden to show that the Dropbox's initial search was government action. Application of this burden here is not straight forward, however, because Balog argues that the private party search exception does not exist under a trespass theory of the Fourth Amendment. Thus, according to Balog, so long as he can prove that the National Center is a government entity or agent, the National Center's warrantless review of his files is the only search that matters. That argument is unpersuasive for the reasons discussed below. And, because Balog does not even try to show that Dropbox's initial search was government action, his motion fails.

## **II. The National Center**

Balog begins his argument by insisting that the National Center is a government entity or agent for the purposes of the Fourth Amendment. The government does not concede the point but argues that the National Center's status is irrelevant. Both are correct.

As it relates to Balog's argument that the National Center is a government entity or agent, he persuasively relies on the Tenth Circuit decision *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016). In *Ackerman*, the Tenth Circuit explained that the National Center qualifies as a government entity because it, *inter alia*, has "law enforcement powers [that] extend well beyond those enjoyed by

private citizens,” *id.* at 1296, and “receives the bulk of its funding from the federal government,” *id.* at 1299. The court reached a similar conclusion in the agency context, explaining that “Congress funded the Center, required [the electronic service provider] to cooperate with it, allowed it to review [the defendant’s] email by excepting it from various federal criminal laws, and statutorily mandated or authorized every bit of its challenged conduct.” *Id.* at 1302. And while the Ninth Circuit has not definitively ruled on this question, it has favorably cited *Ackerman*. See *Rosenow*, 50 F.4th at 729 n.3 (“There is good reason to think that the [National Center] is, on the face of its authorizing statutes, a governmental entity under Fourth Amendment doctrine.”).

Nevertheless, as argued by the government, the private party status at issue here is that of Dropbox, not the National Center. There is no dispute that the National Center’s warrantless search<sup>2</sup> of Balog’s files did not exceed that performed by Dropbox. In fact, Dropbox reviewed 40 files while the National Center reviewed only three. (*See Doc. 29-1.*) Balog does not argue that Dropbox is anything but a private entity, and the Ninth Circuit recently held that electronic

---

<sup>2</sup> Neither party addresses whether Dropbox’s review of Balog’s files constituted a “search” in the first instance. *See United States v. Weber*, 599 F. Supp. 3d 1025, 1032–33 (D. Mont. 2022) (denying suppression motion arising out of an Instagram CyberTip Report on the basis that the defendant failed to show a Fourth Amendment search occurred), *aff’d* 2024 WL 722558 (9th Cir. Feb. 22, 2024) (unpublished). However, at the motion hearing, the government argued for the first time that no “trespass” occurred.

service providers like Dropbox are not government entities or agents simply based on their federal reporting obligations. *See Rosenow*, 50 F.4th at 730–31. Thus, even if the National Center is a government entity or agent, its search fell within the private party search exception as outlined above. Balog maintains, however, that this is beside the point under a trespass theory: “[The National Center] trespassed on Mr. Balog’s papers and effects to search for inculpatory information without a warrant. Under a *Jones* trespass search, [the National Center] is not saved because Dropbox looked at the documents first.” (Doc. 29 at 13.)

### **III. Private Party Search Exception under a Trespass Theory**

Balog insists that the evidence discovered by Dropbox and then sent to the National Center should be suppressed under a “trespass” theory. Fundamentally, Balog argues that the private party search exception does not apply when a physical trespass has occurred, relying primarily on the Supreme Court’s decision in *United States v. Jones*, 565 U.S. 400 (2012). In *Jones*, investigators attached a GPS device to a suspect’s car and tracked the car’s movements for weeks. *Id.* at 402–03. The government argued that no search occurred because the defendant had no reasonable expectation of privacy in his movements on public roads. *Id.* at 406. The Court disagreed, holding that the installation of the GPS device qualified as a “search” because the government “physically occupied private property for the purpose of obtaining information.” *Id.* at 404. According to Balog, “[w]hen

evaluating a trespass search under *Jones*, a prior private frustration of an expectation of privacy has no bearing on whether the government trespassed in order to obtain information. The private party search doctrine should be limited to *Katz* reasonable expectation searches, not *Jones* trespass searches.” (Doc. 29 at 14.) Ultimately, Balog’s trespass argument is not supported by Fourth Amendment authority.

One of the oldest cases addressing the private party search doctrine involved a trespass to property. In *Burdeau v. McDowell*, a 1921 case, papers were taken from the former desk and office of a suspect being investigated for mail fraud by other individuals within the company. 256 U.S. at 473. The Court held that “there was no invasion of the security afforded by the Fourth Amendment against unreasonable search and seizure, as whatever wrong was done was the act of individuals in taking the property of another.” *Id.* at 475.

Likewise, in the Supreme Court’s 1984 *Jacobsen* decision, FedEx employees opened a package, saw it contained a white powdery substance, repacked the materials, and alerted the Drug Enforcement Agency (“DEA”). 466 U.S. at 111. A DEA agent then reopened the package, removed its contents without obtaining a warrant, and found that the white powder was cocaine. *Id.* at 111–12. The Supreme Court upheld the search as constitutional because the agent’s warrantless search fell within the scope of the private search insofar as the

agent “learn[ed] nothing that had not previously been learned during the private search.” *Id.* at 119–20.

More recently, in 2022, the Ninth Circuit upheld a private party search in *Phillips*, where the defendant’s fiancé accessed his laptop without his permission, discovered thousands of images of child pornography, and gave the computer to law enforcement. 32 F.4th at 866–67. In so doing, the fiancé showed the detectives only the images she had already reviewed and investigators used the information gleaned from only those images to get a search warrant for the entire computer. *Id.* at 867. The Ninth Circuit held that the “search was permissible” as the fiancé acted as private party in discovering the contraband and law enforcement did not exceed the scope of her review before obtaining a warrant. *Id.* at 868–69.

But the court in *Phillips* went one step further, explicitly addressing the issue of whether a private party search exception exists under a trespass theory. In doing so, the court recognized that the private party search exception does not permit law enforcement to enter someone’s home without a warrant even on the heels of a private search. *See id.* at 872 (discussing *Stoner v. California*, 376 U.S. 483 (1964), and *United States v. Young*, 573 F.3d 711 (9th Cir. 2009)). But it declined to extend that protection further, explaining that, like *Jacobsen*, *Phillips* “d[id] not involve a warrantless entry into a home or its equivalent.” 32 F.4th at 872. The

court stood by that conclusion even recognizing that computers may contain more personal information than would be discovered in the search of a home. *Id.* at 872–73. Finally, the *Phillips* court specifically addressed a trespass theory under *Jones*, concluding that *Jones* did nothing to undermine the private search exception and once again emphasizing that *Jacobsen* itself was a physical intrusion case. 32 F.4th at 873–74; *see also United States v. Totsi*, 733 F.3d 816, 818–19 (9th Cir. 2013) (upholding a search that occurred after a computer technician discovered child pornography on a device).

A hypothetical used during the hearing provides a good example of why Balog’s argument fails. Defense counsel argued that if a cleaning person entered a residence and found a pound of cocaine, that cleaning person could not take law enforcement back into the residence to show them the cocaine. The Court agrees. However, if the cleaning person took the cocaine with them and turned it over to law enforcement, there is no question under existing authority that law enforcement could use that privately-obtained cocaine to seek a search warrant for the residence. *See Coolidge*, 403 U.S. at 489 (holding that when a private individual provides law enforcement with evidence, “it [i]s not incumbent on the police to stop [the private person] or avert their eyes”).

Ultimately, even if the search at issue here is considered a “trespass,” *see United States v. Weber*, 599 F. Supp. 3d 1025, 1034 (D. Mont. 2022) (“In the wake

of *Jones*, the Supreme Court has routinely applied the *Katz* test, at the expense of the *Jones* test, in intrusions into cyberspace.”), the private party search exception applies. Consistently, both the National Center and Detective Harris’s warrantless searches of Balog’s files were permissible so long as they did not exceed the scope of Dropbox’s initial search.<sup>3</sup> Balog makes no argument on that point. As such, his motion can be denied without addressing the government’s alternative arguments.

*See Weber*, 599 F. Supp. 3d at 1032 (“And because nobody asserts Instagram is a state actor, [the defendant] cannot complain that its actions violated the Fourth Amendment, because the Fourth Amendment does not apply to private conduct.”). Nonetheless, because the government’s alternative arguments also support denying Balog’s motion, they are discussed below.

#### **IV. Alternative Grounds**

---

<sup>3</sup> The Ninth Circuit recently held in an unpublished memorandum disposition that it “need not decide whether the trespass theory applies to searches of electronic information, because the disclosure of [the defendant]’s information by [the electronic service provider] to the government was licensed pursuant to the [service provider]’s Terms of Service.” *United States v. Weber*, 2024 WL 722558, at \*1 (9th Cir. Feb. 22, 2024). The court went on to state, however, that it “offer[ed] no opinion on more general terms of service, nor [did it] consider a license’s effect under a reasonable-expectation-of-privacy theory.” *Id.* Neither issue forms the basis of either Balog’s or the government’s argument here. Indeed, Dropbox’s Terms of Service merely state that third party disclosure may occur if “reasonably necessary to comply with applicable laws,” (*see* Doc. 29-3), and Balog specifically eschews a “reasonable expectation of privacy” analysis, *see United States v. Sarkisian*, 197 F.3d 966, 986 (9th Cir. 1999) (placing the burden on the defendant to show that he has a “legitimate expectation of privacy” in the items seized or area searched).

The government argues that even if the National Center is a government entity or agent and its search of Balog's Dropbox account was infirm, suppression is not appropriate because: (1) Detective Harris did not rely on the information from the National Center's review in his warrant application, (2) even if the minimal information from the National Center was excised from the warrant, probable cause would lie, and (3) the "good faith" exception should apply. These arguments are also persuasive.

#### **A. Detective Harris's Warrant Application**

As argued by the government, Detective Harris's warrant application relies primarily, although not exclusively, on the information gleaned by Dropbox, not the National Center. Harris recounts the account information provided by Dropbox and explains Dropbox's categorization process. (*See* Doc. 32-1 at 2–3.) The warrant application did not reference the three files reviewed by the National Center. Nonetheless, the application does mention the National Center's automated categorization process, with reference to "hash matches" to known child pornography. (*See id.* at 3.) While the government's description of this information as "tangential," (Doc. 32 at 14), may understate its relevance, probable cause would exist in its absence.

"Probable cause to search a location exists if, based on the totality of the circumstances, there is a fair probability that evidence of a crime may be found

there.” *United States v. Perkins*, 850 F.3d 1109, 1119 (9th Cir. 2017) (internal quotation marks omitted). “The duty of the reviewing court is simply to ensure that the magistrate had a substantial basis for concluding that probable cause existed.” *United States v. Thompson*, 751 F.2d 300, 301–02 (8th Cir. 1985). The magistrate’s determination of probable cause “should be paid great deference.” *United States v. Gourde*, 440 F.3d 1065, 1069 (9th Cir. 2006). A search warrant is not “rendered invalid merely because some of the evidence included in the affidavit is tainted.” *United States v. Nora*, 765 F.3d 1049, 1058 (9th Cir. 2014). “The warrant remains valid if, after excising the tainted evidence, the affidavit’s remaining untainted evidence would provide a neutral magistrate with probable cause to issue a warrant.” *Id.* (internal quotation marks omitted).

As mentioned above, the only information in Detective Harris’ warrant application that implicates the National Center’s interaction with Balog’s specific files reads as follows:

Additionally, NCMEC automates a categorization of the files based on [the National Center]’s review of uploaded files in the report OR a “Hash Match” of one or more uploaded files to visually similar files that were previously viewed and categorized by [the National Center]. [The National Center] categorized the files as “Apparent Child Pornography[,]” “CP (Unconfirmed)” and “Child Unclothed[.]”

(Doc. 32-1 at 3.) As argued by the government, removing this information leaves probable cause “intact.” (Doc. 32 at 16.) The remaining information in the affidavit/CyberTip Report shows that Dropbox reported 40 images of potential

child sexual abuse material and Dropbox categorized that material itself as depicting specific types of sexually explicit material. (*See Doc. 29-1 at 4–14.*) And while the physical location of the IP address was added by the National Center after the fact, the IP address itself was provided by Dropbox; the National Center merely used a publicly-available database to determine the geographic location of that address. (*See Doc. 29-1 at 3, 15.*) Balog’s attempt to attribute all the substantive contents of the CyberTip Report to the National Center is unavailing.

#### **B. “Good Faith” Exception**

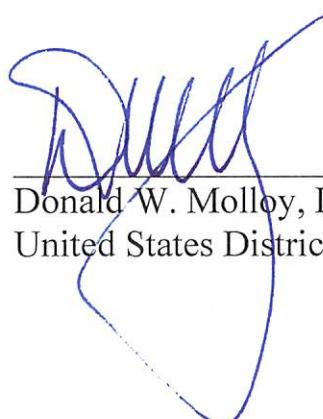
“The Fourth Amendment contains no provision expressly precluding the use of evidence obtained in violation of its commands.” *United States v. Leon*, 468 U.S. 897, 906 (1984). “The good-faith exception precludes the suppression of evidence seized by officers who acted ‘in objectively reasonable reliance’ on a search warrant that is later declared invalid.” *United States v. Artis*, 919 F.3d 1123, 1133 (9th Cir. 2019) (quoting *Leon*, 468 U.S. at 922). This exception may be triggered if a search warrant is issued based on evidence illegally obtained as a result of constitutional errors by the police. *Id.* The relevant question is “whether the police misconduct that led to the discovery of the illegally obtained evidence is itself subject to the good-faith exception. If it is, suppression of the evidence seized pursuant to the warrant will not be justified.” *Id.* In *Weber*, a recent

unpublished decision, the Ninth Circuit held that the good faith exception applied where an officer reasonably relied on the information contained in a CyberTip Report and whose subsequent search did not exceed the scope of the original private party search. *United States v. Weber*, 2024 WL 722558, at \*2 (9th Cir. Feb. 22, 2024). That is the case here.

#### CONCLUSION

Based on the foregoing, IT IS ORDERED that Balog's motion to suppress (Doc. 28) is DENIED.

DATED this 20<sup>th</sup> day of May, 2024.



15:31 P.M.  
Donald W. Molloy, District Judge  
United States District Court